

ROBERT WAGGENER - SBN: 118450
LAW OFFICE OF ROBERT WAGGENER
214 Duboce Avenue
San Francisco, California 94103
Phone: (415) 431-4500
Fax: (415) 255-8631
E-Mail: rwlaw@mindspring.com
Attorney for Defendant RUSSELL T. OTT

MARCIA ANN MORRISSEY - SBN: 66921
LAW OFFICE OF MARCIA ANN MORRISSEY
11400 W. Olympic Blvd., STE 1500
LOS ANGELES, CA 90064
Phone: (310) 399-3259
Fax: (310) 392-9029
E-mail: morrisseyma@aol.com
Attorney for Defendant RUSSELL TAYLOR OTT

JOHN T. PHILIPSBORN - SBN 83944
Law Offices of JOHN T. PHILIPSBORN
507 Polk Street, Suite 350
San Francisco, CA 94102
(415) 771-3801
jphilipsbo@aol.com
Attorney for BRIAN WAYNE WENDT

RICHARD G. NOVAK - SBN 149303
P.O. Box 5549
Berkeley, Ca 94705
(626) 578-1175
Richard@RGNLaw.com
Attorney for JONATHAN NELSON

JAI M. GOHEL SBN 170782
819 Eddy Street
San Francisco, CA 94109
(415) 771-6714
Jaigohel@rocketmail.com
Attorney for JONATHAN NELSON

K. ALEXANDRA McCLURE - SBN 189679
214 Duboce Avenue
San Francisco, CA 94103
(415) 814-3397
alex@alexmccclurelaw.com
Attorney for BRIAN WAYNE WENDT

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

RUSSELL TAYLOR OTT,

Defendant.

No. CR 17 00533 EMC

**NOTICE OF JOINT GROUP ONE
DEFENSE OBJECTION TO UNITED
STATES' CERTIFICATES OF
AUTHENTICITY UNDER FRE 902(14)**

**Dept: The Honorable Edward M. Chen
United States District Judge**

**TO: THE UNITED STATES ATTORNEY FOR THE NORTHERN DISTRICT OF
CALIFORNIA; ASSISTANT UNITED STATES ATTORNEYS KEVIN BARRY,
AJAY KRISHNAMURTHY AND LINA PENG; AND TO THE CLERK OF THE
ABOVE-ENTITLED COURT:**

**JOINT GROUP ONE DEFENSE OBJECTION
TO ELECTRONIC DEVICE AUTHENTICATION**

I. INTRODUCTION AND SUMMARY OF THE OBJECTIONS

The government has filed three documents entitled United States' Notice of Certificate of Authenticity Under FRE 902(14). ECF 2714, 2719, 2720. Each notice relates to a different FBI employee: forensic examiner Beth Marquis Mauldin, FBI Supervisory Special Agent and Digital Extraction Technician Alex Mah, and FBI Special Agent and Digital Extraction Technician Michael Mansuy. Each certificate contains a declaration from the examiner/technician as to their extraction of various electronic devices connected to this case, each identified by an Extraction Identifier number, SVE#####: Mauldin - 11 devices (5 phones, 6 hard drives or thumb drives), Mah - 4 devices (hard drives and thumb drives), Mansuy - 2 devices (hard drives). None of these technicians have testified or been noticed to testify.¹ The government is obviously relying on the three certificates and declarations to authenticate the electronic devices and all of the chosen exhibits picked from the mountain of data. The defense objects.

II. ARGUMENTS AND AUTHORITIES

This Court should reject the government's attempts to authenticate certain evidence pursuant to Federal Rule of Evidence 902 (14) for several reasons. First, the government has failed to provide reasonable notice—the government waited until over one month into trial, such notice is not reasonable under the circumstances. The certificates were filed last week. Second, the government has failed to comply with the text of Section 902(14) by failing to establish that the witness is qualified to render the proffered opinion. Third, as provided by the notes, “A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record of the certifying person testified, then authenticity is not established under this Rule.” Here, the government even failed to comply with the minimum of the Rule, which is to provide the actual

¹ Witnesses Mauldin and Mah are on the government's witness list. Witness Mansuy is not.

1 hash value which would allow the defense to conduct a similar comparison. The documentation of
 2 the certificates is absolutely minimal. Fourth, the notice fails to comply with Rule 902(11), as
 3 required by Section 902(14), which provides that the notice must comply with Rule
 4 803(6)(A)-(C), the business record exception to the hearsay rule. The government's failure to do
 5 so is disqualifying. Fifth, to the extent Rule 902(14) allows the government in a criminal case to
 6 admit evidence in the absence of a witness, it violates the accused rights under the Fifth and Sixth
 7 Amendments of the constitution. Thus, this Court should strike the government's notice and
 8 exclude or strike admission of the evidence derived from the various electronic devices because
 9 the government failed to comply with Rule 902, and the admission of such evidence is
 10 unconstitutional.

11 One issue for the Court to understand is that these various electronic devices contain
 12 hundreds of gigabytes of data. The trial in this case has provided only limited context or
 13 specificity of origin as to the various photographs, videos, documents, and emails culled from
 14 these various devices. Blanket authentication of all these items by means of three bare bones
 15 certificates and declarations, not even identifying the amount of data extracted or the source and
 16 chain of custody of the various evidence exhibits, is fundamentally unfair to a criminal defendant.²

17 There is very little case law as to FRE 902(14). One criminal case in the Sixth Circuit that
 18 passed muster as to a certificate of authenticity involved a single cell phone of the defendant
 19 where the certificate of authenticity was filed pretrial. *United States v. Dunnican*, 961 F.3d
 20

21 ² The legislative history of FRE 902(14) is instructive. The government has violated the
 22 terms and elements of the rule, as well as its general purpose.

23 "A certification under this Rule can only establish that the proffered item is authentic.
 24 The opponent remains free to object to admissibility of the proffered item on other
 25 grounds—including hearsay, relevance, or in criminal cases the right to confrontation. For
 26 example, in a criminal case in which data copied from a hard drive is proffered, the defendant
 27 can still challenge hearsay found in the hard drive, and can still challenge whether the
 28 information on the hard drive was placed there by the defendant.

A challenge to the authenticity of electronic evidence may require technical information
 about the system or process at issue, including possibly retaining a forensic technical expert; such
 factors will affect whether the opponent has a fair opportunity to challenge the evidence given the
 notice provided."

1 859(6th Cir. 2020) Our case is an entirely different animal where the notices were filed in the
2 midst of trial as to the wholesale data in multiple devices from a range of devices attributed to
3 multiple people and locations, and non-defendants.

4
5 Dated: May 25, 2022

Respectfully submitted,

6 /s/

7 ROBERT F. WAGGENER
8 MARCIA M. MORRISSEY
9 JOHN T. PHILIPSBORN
K. ALEXANDRA McCLURE
JAI M. GOHEL
RICHARD G. NOVAK

10
11 By: /s/ Robert F. Waggener
12 ROBERT F. WAGGENER
On Behalf of Group One Defense